ABSTRACT

Data are converted between an unencrypted and an encrypted format according to the Rijndael algorithm, including a plurality of rounds. Each round is comprised of fixed set of transformations applied to a two-dimensional array, designated state, of rows and columns of bit words. At least a part of said transformations are applied on a transposed version of the state, wherein rows and columns are transposed for the columns and rows, respectively.

(Figure 6)